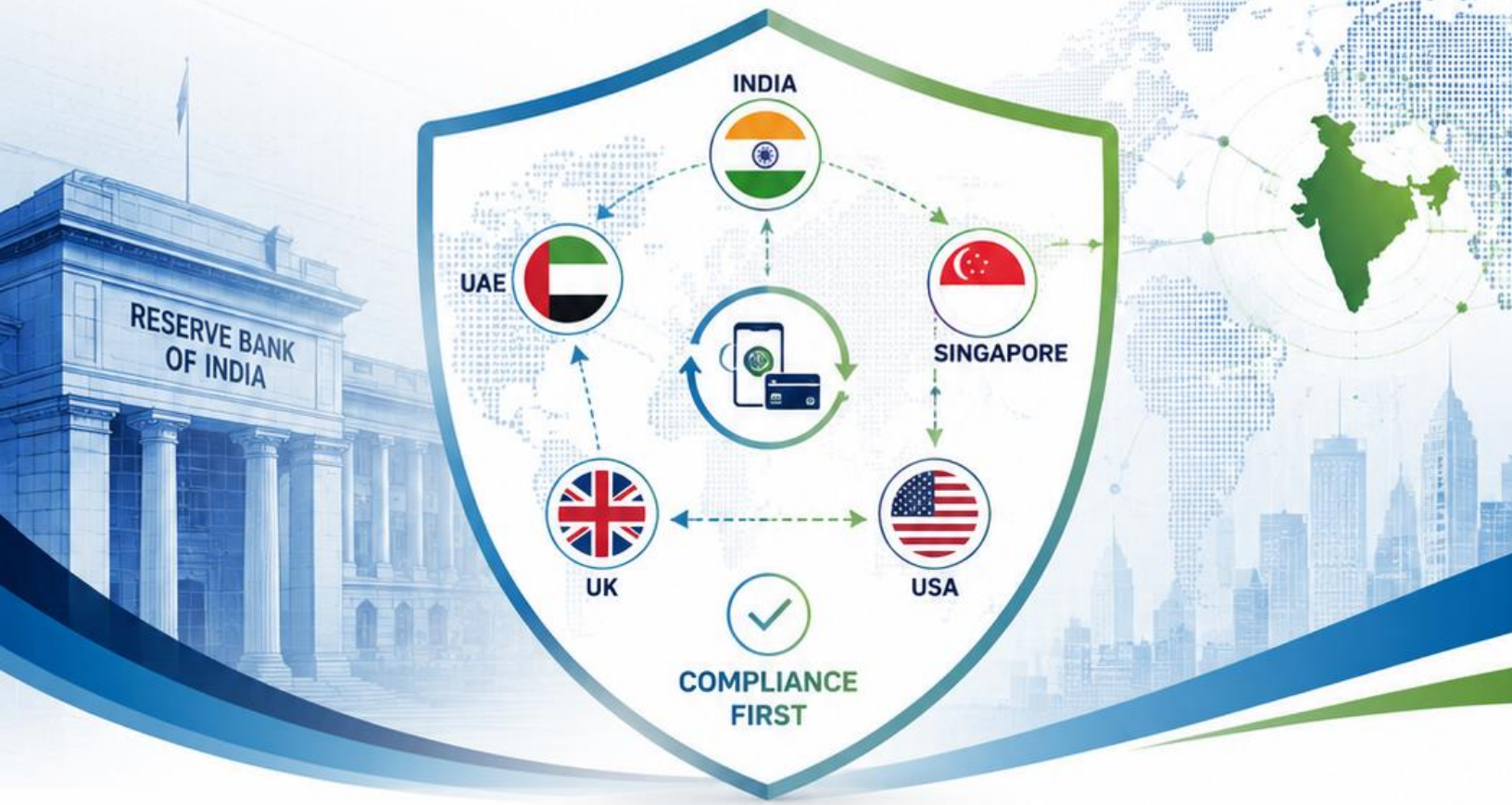
COMPLY GLOBALLY

An Initiative of **Connect Ventures Inc, USA**

COMPLY GLOBALLY INSIGHTS SERIES

Why Your Fintech's Cross-Border Payment Flow Might Be an Unregistered Money Transfer Operation

A Practical Compliance Guide Covering
FEMA*, *PSS Act*, *PMLA*, *Income Tax Act
*and **RBI** Regulatory Framework*



Dr. Anil Gupta
Chairman, Connect Ventures Group
Mentor of Change, **NITI Aayog**

COMPLIANCE **FOCUSED** | GLOBAL **PERSPECTIVE** | REGULATORY **CLARITY** | PRACTICAL **GUIDANCE**

Introduction: The Trap Nobody Sees Coming

“We’re just a technology platform. We don’t move money.”

This is one of the most common — and the most expensive — statements a fintech founder can make. The moment your platform facilitates the movement of value between a person in India and someone outside it, you are in the cross-border money transfer business. And that business is one of the most heavily regulated activities in India’s financial ecosystem — policed by at least five major legal frameworks simultaneously.

India has a dense regulatory web that applies to cross-border payment flows:

- **Foreign Exchange Management Act, 1999 (FEMA)** — governs who can deal in foreign exchange and under what conditions
- **Payment and Settlement Systems Act, 2007 (PSS Act)** — governs who can operate a payment system
- **Prevention of Money Laundering Act, 2002 (PMLA)** — applies KYC and AML obligations
- **Income Tax Act, 1961** — governs withholding tax, TDS on VDAs, and taxation of cross-border income
- **RBI Master Directions** — prescribe operating standards for payment aggregators, money changers, and authorised dealers

Any one of these can trip you up. All five together can shut you down. This article walks you through each framework in plain language — with practical tips, specific legal references, real-world examples, and clear advisories about what to watch for and what to do.

> **ADVISORY: Who Should Read This?**
>
> This guide is written for fintech founders, CFOs, product managers, and legal advisors dealing with cross-border payments involving Indian residents or Indian entities. If your product has any feature that allows money or financial value to cross an Indian border — inward or outward — every section of this article is relevant to you.

Part 1: What Is an "Unregistered Money Transfer Operation" — In Plain Language?

Let's start with the term nobody defines clearly.

Under Section 4 of the Payment and Settlement Systems Act, 2007: No person — other than the Reserve Bank of India — can commence or operate a payment system without prior authorisation from the RBI. The Act defines a "payment system" broadly to include any system that enables payment to be effected between a payer and a beneficiary, including clearing, payment, or settlement services.

Under Section 3 of FEMA, 1999: No person shall deal in, transfer, purchase, or sell any foreign exchange or foreign security to or for a person resident outside India without being an Authorised Person recognised by the RBI.

So in plain language: if your platform moves, facilitates, pools, processes, converts, or settles money that crosses India's border — and you do not hold the appropriate licence from the RBI — you are operating an unregistered money transfer operation. The name on your app does not matter. Your incorporation certificate does not matter. What matters is the function your system performs.

LAW REFERENCE: Key Statutory Provisions

PSS Act, 2007 — Section 26: Operating an unauthorised payment system can attract imprisonment up to two years, or a fine up to INR 10 lakhs, or both — PLUS INR 10,000 per day for each day the violation continues.

FEMA, 1999 — Section 13: Violation of FEMA attracts a civil penalty of up to three times the sum involved, or INR 2 lakhs per contravention (whichever is higher). The Enforcement Directorate can also attach assets.

PMLA, 2002 — Section 4: Money laundering (which includes facilitating unlawful money movement) is punishable by rigorous imprisonment of 3 to 7 years, extendable to 10 years in certain cases, plus fine.

PRACTICAL TIP

The "Am I moving money?" Test: Ask this question about every flow in your product: "Does this transaction involve the movement of financial value between a person in India and a person or entity outside India?" If yes, FEMA applies. If sometimes, you still need legal review. If you are unsure, that uncertainty IS your compliance gap.

Part 2: FEMA 1999 — The Law That Governs Every Cross-Border Rupee

The Foreign Exchange Management Act, 1999 replaced the old Foreign Exchange Regulation Act (FERA) and came into force on 1 June 2000. While FERA was a penal law (where the accused had to prove innocence), FEMA is primarily a civil compliance law — but RBI and Enforcement Directorate enforcement has grown significantly more aggressive since 2017.

Here are the provisions every fintech leader must understand:

Section 2: The Wide Definition of "Foreign Exchange"

FEMA defines "foreign exchange" to include foreign currency, all deposits, credits and balances payable in foreign currency, drafts, travellers' cheques, letters of credit, and bills of exchange expressed in Indian currency but payable in foreign currency. This definition is intentionally broad. The moment a transaction on your platform involves any of these instruments — you are in FEMA territory.

Section 3: The Core Prohibition — No Unauthorised Dealing

Section 3 makes it unlawful for any person to:

- Deal in, transfer, purchase, or sell any foreign exchange or foreign security without being an Authorised Person
- Make any payment to, or for the credit of, any person resident outside India in any manner — unless through authorised channels
- Receive any payment from a person resident outside India through channels other than Authorised Persons
- Enter into any financial transaction in India as consideration for or in association with acquisition or creation of assets outside India, without RBI permission

Section 4: Holding Foreign Exchange

No person resident in India can acquire, hold, own, possess, or transfer any foreign exchange, foreign security, or immovable property outside India — except as provided under FEMA. This section is particularly relevant for fintech platforms that allow Indian residents to hold foreign-currency-denominated balances or stablecoins.

Section 6: Capital Account Transactions

Capital account transactions — which broadly means transactions that alter the assets or liabilities of a person outside India — require specific RBI permission unless explicitly permitted under Schedule III of FEMA (Capital Account Transactions) Rules. For fintechs handling equity investments, overseas direct investment, or external commercial borrowings, this section is critical.

Section 10: The Authorised Person Framework

Only persons authorised by the RBI can deal in foreign exchange. The three categories of Authorised Persons are:

- **AD Category I Banks:** Scheduled commercial banks. They can handle all permissible foreign exchange transactions and are the primary banking partners for cross-border fintech flows.
- **AD Category II:** Select cooperative banks, Regional Rural Banks, and urban cooperative banks. Limited to specific forex transactions — encashment, limited remittances.
- **AD Category III (Full-Fledged Money Changers — FFMCs):** Licensed to buy and sell foreign currency notes, coins, and travellers' cheques. Cannot handle all remittance types.

> **CAUTION: Your Bank API Is Not a Licence**
>
> A common misconception: "We use XYZ Bank's payment API, so their licence covers us." It does not — or at least not automatically. Using a bank's API makes you a technology service provider to that bank, not an authorised entity yourself. For the bank's authorisation to extend to your platform, you need a formal agreement that explicitly identifies your role, allocates regulatory responsibility, and specifies KYC and AML obligations. Get this agreement reviewed by a lawyer who understands payment system regulation.

Part 3: The Settlement Layer Trap — Where Most Founders Get Caught First

This is the most common compliance gap in Indian fintech. A founder builds a product — a B2B invoicing tool, a freelancer payment app, a marketplace — and assumes that because a licensed bank processes the actual payment, the regulatory burden sits entirely with the bank. It does not.

Here is the scenario that trips most platforms:

Your app collects payment from a global client in USD. The funds sit in your company's current account for anywhere from a few hours to a few days. You then convert and pay the Indian beneficiary in INR. In your view: you are a technology intermediary. In the RBI's view: you may be operating an unlicensed Payment Aggregator.

Who Is a Payment Aggregator Under RBI's Master Direction (2020)?

Under the RBI's Master Direction on Payment Aggregators and Payment Gateways (dated 17 March 2020, updated in 2023), a Payment Aggregator (PA) is any entity that facilitates e-commerce merchants to accept payment instruments from customers by aggregating and settling funds. If your platform:

- Collects payment from one party (payer)
- Pools those funds — even briefly — in any account

- Disburses those funds to another party (merchant or beneficiary)

...you may be a PA, regardless of what your product is called.

Payment Aggregator Licence Requirements

As per the RBI's PA guidelines, entities operating as Payment Aggregators must:

1. Obtain a specific Payment Aggregator licence from the RBI's Department of Payment and Settlement Systems (DPSS)
2. Maintain all customer funds in a Nodal Account or Escrow Account held with a scheduled commercial bank — not in their own operating account
3. Prohibit commingling of customer funds with company funds — at any point, for any duration
4. Achieve a minimum net worth of INR 25 crore by 31 March 2023, and INR 50 crore by 31 March 2026
5. Implement full merchant KYC: physical address verification, financial due diligence, and ongoing monitoring
6. Maintain a Board-approved fraud risk management policy and a customer grievance redressal mechanism
7. Submit to regular RBI audits

> **CAUTION: The Two-Hour Float Problem**
>
> A critical point that surprises most founders: the RBI does not recognise a minimum holding period below which you are exempt from PA rules. If customer funds pass through your own current account — even for two hours, even for two minutes — before reaching the beneficiary, you are likely in violation of the nodal/escrow account requirement. The fix is not to shorten the float. The fix is to eliminate it — route customer funds directly through the licensed nodal account structure from the moment they are received.

The Money Transfer Service Scheme (MTSS) — A Separate Framework for Inward Remittances

MTSS is an RBI-authorised framework under which inward remittances (money coming into India from abroad, primarily for personal purposes) are processed. MTSS is used by global money transfer operators like Western Union and MoneyGram, which appoint RBI-authorised Indian agents to deliver cash to beneficiaries.

Key MTSS restrictions:

- Maximum per-transaction limit: USD 2,500
- Maximum 30 remittances per year from a single sender to a single receiver
- Payment only in Indian Rupees — no foreign currency delivery to the beneficiary
- Permitted purposes: family maintenance, travel expenses, medical expenses — not business payments
- Only RBI-authorised MTSS agents can operate within this framework

ADVISORY

If your fintech app helps Indian individuals receive personal money from abroad — from family members, freelance clients, or diaspora transfers — you are likely in MTSS territory. You must either be a licensed MTSS agent or formally partner with one. There is no "technology platform" exemption to this licensing requirement. A product that looks like a consumer app but performs MTSS functions without authorisation is a PSS Act violation, not just a regulatory technicality.

Part 4: The Liberalised Remittance Scheme (LRS) — Hidden Obligations for Outward Payment Platforms

The Liberalised Remittance Scheme (LRS) is one of FEMA's most practically important provisions for consumer-facing fintechs. It allows Indian resident individuals to remit up to USD 250,000 per financial year for any permissible current or capital account purpose — education, travel, foreign stock investment, maintenance of relatives abroad, etc.

If your platform allows Indian residents to send money abroad for any purpose, here is what you are legally required to do:

8. Collect purpose-of-remittance documentation from each user, as specified by RBI (Form A2 declarations for AD banks)
9. Ensure the transaction flows through an AD Category I bank, which will report each LRS transaction to the RBI with the user's PAN
10. Integrate TCS (Tax Collected at Source) at the applicable rate into your payment flow
11. Ensure no single user exceeds the USD 250,000 annual cap — noting that all LRS remittances from a user across ALL platforms are aggregated by PAN

TCS Rates on LRS Remittances (Effective October 2023)

The Finance Act 2023 significantly revised TCS rates on LRS. As of 1 October 2023:

- **Education (funded by education loan from financial institution):** 0.5% TCS
- **Education / Medical purposes:** 5% TCS
- **All other LRS purposes (travel, foreign investment, gifting, maintenance):** 20% TCS

CAUTION: 20% TCS — A Major Cash Flow Impact

If a user remits INR 5 lakhs abroad for overseas stock investment through your platform, they must pay an additional INR 1 lakh as TCS at source. This is not a penalty — TCS is creditable against the user's tax liability. But it is a significant upfront cash outflow that your UX and product flow must make visible to users BEFORE they initiate the transaction. Failure to collect and deposit TCS makes your platform the liable party — not the user.

What LRS Does NOT Permit

The following outward remittances are not allowed under LRS, and your platform must screen for these:

- Trading in foreign exchange abroad (except through instruments specifically permitted by RBI)
- Purchasing lottery tickets, sweepstakes, proscribed magazines, or forbidden items
- Payment of call margins or margin calls to foreign exchanges directly
- Capital account transactions not explicitly permitted by the RBI under Schedule III of FEMA (CA Transaction) Rules
- Remittances to countries notified as non-cooperative by the Financial Action Task Force (FATF)

PRACTICAL TIP

Build a per-user LRS Tracker: Your platform should maintain a running LRS utilisation record for each user (mapped to PAN), integrated with your AD bank's reporting. Flag transactions when a user's cumulative annual remittance approaches USD 200,000 — giving them and your compliance team a buffer before the USD 250,000 cap is hit. Also screen for structuring behaviour: a single source sending multiple smaller transactions through multiple users to avoid the reporting threshold is a PMLA red flag, not just an LRS issue.

Part 5: DTAA, Permanent Establishment, and Why Your Singapore Entity Is Not a Shield

India has signed Double Tax Avoidance Agreements (DTAAs) with over 90 countries. These are powerful instruments — when used on the foundation of genuine business substance. The problem is that many fintech founders use them as paper structures to route income away from India, without understanding that India's tax law has robust tools to look through such arrangements.

Understanding Permanent Establishment (PE) — Article 5 of Most DTAAs

A Permanent Establishment (PE) is defined in Article 5 of the India-Singapore DTAA (and virtually every other treaty India has signed) as a fixed place of business through which the business of an enterprise is wholly or partly carried on. This includes branches, offices, factories, and construction sites lasting more than six months.

But the most dangerous PE for fintechs is the Dependent Agent PE. Under Article 5(5) of the India-Singapore DTAA, an enterprise has a PE where a person in India habitually exercises an authority to conclude contracts on behalf of the enterprise, even if that person is not a formal

employee. Your Bengaluru team that negotiates deals, services clients, and effectively runs operations for your Singapore entity? They are dependent agents.

Real-World Example — PayBridge (Illustrative): Arjun founds a payments API startup. He incorporates a Singapore parent, keeps 35 engineers in Koramangala, and routes all global revenue through Singapore for a lower headline tax rate. His Indian team negotiates contracts, finalises commercial terms, and services all clients. The Indian tax authority can — and under audit, often does — argue that PayBridge has a dependent agent PE in India, and that a material portion of Singapore-booked income is attributable to that PE. The entire tax-efficiency structure collapses, with penalties for under-reporting stacked on top.

Significant Economic Presence (SEP) — Section 9(1)(i) of the Income Tax Act

India introduced the SEP rule via the Finance Act 2018, effective from Assessment Year 2022-23. Under SEP, even without a physical presence in India, a non-resident entity has a deemed business connection in India (and therefore taxable income in India) if:

- Revenue from transactions with Indian users exceeds INR 2 crore in a financial year, OR
- The non-resident engages in systematic and continuous soliciting of business through digital means with 3 lakh or more users in India

For a Singapore-incorporated fintech with a significant Indian user base, this is a material and immediate risk. The profits attributable to this deemed PE become taxable in India.

GAAR — Sections 95–102 of the Income Tax Act

India's General Anti-Avoidance Rules (GAAR) came into force in April 2017. Under GAAR, the Income Tax Authority can disregard, recharacterise, or consolidate any arrangement that is an "impermissible avoidance arrangement" — defined as an arrangement whose main purpose is to obtain a tax benefit. The four tests applied under GAAR are:

12. Is the arrangement not at arm's length?
13. Does it misuse or abuse a provision of the tax treaty?
14. Does it lack commercial substance (i.e., has no real business purpose beyond tax)?
15. Is it carried out in a manner not ordinarily employed for bona fide business?

A Singapore shell with no employees, no decision-making authority, no IP ownership, and no meaningful business activity — that merely invoices Indian clients — will fail every one of these tests.

Place of Effective Management (POEM) — Section 6(3) of the Income Tax Act

For foreign companies, Section 6(3) deems a company as a tax resident of India if its Place of Effective Management (POEM) is in India. POEM means the place where key management and commercial decisions necessary for the conduct of the entity's business are, in substance, made. If your Singapore board meets twice a year for 30 minutes and everything else happens in India, the Indian tax authority will argue POEM — making your Singapore entity a de facto Indian tax resident.

ADVISORY: What Genuine Substance Looks Like

To maintain a legitimate offshore holding structure, you need these elements to be genuinely present in the holding company's jurisdiction:

(a) Board composition and residency: A majority of directors must be resident in the holding company's jurisdiction and attend board meetings physically there.

(b) Decision-making: Key commercial decisions — pricing, product strategy, major contracts — must be made and recorded in that jurisdiction.

(c) Employees: The entity must have qualified, salaried employees in that jurisdiction performing real functions.

(d) Economic substance: Singapore's Economic Substance Act (and similar laws in UAE, Cayman Islands, etc.) now require businesses to demonstrate economic substance as a condition of enjoying low-tax rates. This is not optional. A Singapore company that fails the substance test faces penalties in Singapore AND cannot claim DTAA benefits in India.

Part 6: PMLA 2002 — The Compliance Obligation Most Fintechs Overlook

The Prevention of Money Laundering Act, 2002 (PMLA) is not merely a law targeting criminals laundering proceeds of crime. Since 2019 and especially after 2023 amendments, it is an extensive operational compliance framework that applies directly to payment system operators, payment aggregators, and virtual digital asset (VDA) exchanges — all of which are now explicitly included as "Reporting Entities" under the PMLA.

Your Obligations as a Reporting Entity

If your fintech qualifies as a Reporting Entity under PMLA, you must:

16. **Customer Due Diligence (CDD):** Conduct KYC at onboarding — PAN/Aadhaar for Indian residents, equivalent documentation for non-residents. Verify name, address, identity, and nature of business relationship.
17. **Enhanced Due Diligence (EDD):** For high-value transactions, Politically Exposed Persons (PEPs), and transactions from FATF-listed high-risk jurisdictions — collect detailed source-of-funds documentation, conduct deeper background checks, and obtain senior management approval.
18. **Record Maintenance (Section 12 of PMLA):** All transaction records must be maintained for five years from the date of transaction. For ongoing business relationships, five years from the date the relationship ends. These records must be readily available to the FIU-IND or other investigating authorities.
19. **Reporting to FIU-IND:** Report to India's Financial Intelligence Unit as follows:
    Cash Transaction Reports (CTRs): Cash transactions above INR 10 lakhs
    Suspicious Transaction Reports (STRs): Any transaction suspected of involving money laundering — regardless of amount

Cross-Border Wire Transfer Reports (CCTRs): International wire transfers of USD 25,000 or more (or equivalent in any currency)

20. **Appoint a Principal Officer:** A named senior officer responsible for PMLA compliance must be designated and their details filed with FIU-IND. This person is personally responsible for ensuring timely reporting and can be held liable for non-compliance.
21. **Annual AML Audit:** Conduct an independent audit of your AML/CFT (Anti-Money Laundering / Combating the Financing of Terrorism) framework annually.

CAUTION: Double Jeopardy — FEMA + PMLA Together

The Enforcement Directorate has jurisdiction over BOTH FEMA violations and PMLA offences. When a cross-border payment platform operates without authorisation, a single compliance failure can trigger FEMA penalties (civil) AND PMLA prosecution (criminal). This double-jeopardy risk is not theoretical — the ED has pursued both tracks simultaneously in several fintech enforcement actions. Assets can be attached under PMLA even before a conviction.

FIU-IND Penalties (Section 13, PMLA): INR 10,000 to INR 1,00,000 per day for each day of non-compliance. Repeat violations attract mandatory escalation to the Director of FIU-IND for formal adjudication.

PRACTICAL TIP

PMLA Compliance Basics You Can Implement Today: (1) Identify whether your entity is a Reporting Entity — if you process cross-border payments, you almost certainly are. (2) Appoint and register your Principal Officer with FIU-IND at goaml.fiu.gov.in. (3) Implement automated transaction monitoring with threshold alerts. (4) Screen all users against OFAC, UN Security Council, and RBI sanction lists. (5) Conduct a gap assessment against RBI's KYC Master Direction (January 2020, as amended).

Part 7: Crypto, Stablecoins, and Virtual Digital Assets — No Regulatory Safe Harbour Exists

The Supreme Court of India's 2020 ruling in Internet and Mobile Association of India v. Reserve Bank of India set aside the RBI's 2018 banking ban on crypto businesses. This created a dangerous misconception: that crypto in India is unregulated. It is not. The ruling merely struck down the specific circular — it did not create a regulatory exemption. VDA platforms now face a more complex, multi-framework compliance environment than before.

What Is a Virtual Digital Asset (VDA) Under Indian Law?

Section 2(47A) of the Income Tax Act, 1961 (inserted by the Finance Act 2022) defines VDA to include any information, code, number, or token generated through cryptographic means or otherwise that provides a digital representation of value. This includes:

- Cryptocurrencies (Bitcoin, Ethereum, and all other tokens)
- Non-fungible tokens (NFTs)
- Stablecoins (including USD-pegged stablecoins like USDT, USDC)
- Any other digital asset notified by the Central Government

The definition is intentionally broad. Most tokens, regardless of labelling, fall within VDA.

Income Tax Obligations for Fintechs Handling VDAs

Section 115BBH — Flat 30% Tax on VDA Gains: All income from transfer of VDA is taxed at a flat 30% with no deduction allowed except the cost of acquisition. No loss from VDA transactions can be offset against any other income head. Gift of a VDA above INR 50,000 is taxable as income in the recipient's hands.

Section 194S — 1% TDS on Every VDA Transfer: Any person responsible for making payment on transfer of a VDA must deduct 1% TDS before releasing the payment. For fintech platforms that facilitate VDA trades, exchange, or transfers, the platform is the deducting entity. If the platform fails to deduct and deposit TDS, the liability — including interest and penalty — falls on the platform, not the user.

LAW REFERENCE: VDA and FEMA — The Stablecoin Problem

A USD-pegged stablecoin held by an Indian resident is, in economic substance, a USD-denominated foreign exchange asset. Under Section 4 of FEMA, an Indian resident cannot hold foreign exchange without authorisation. If your platform allows Indian users to maintain stablecoin balances denominated in USD or any other foreign currency, you may be facilitating a FEMA violation for each such user.

Further, if users use stablecoins to effectively remit value abroad beyond their LRS cap (USD 250,000/year), this constitutes an LRS violation — and the platform enabling it shares the regulatory exposure. The FEMA view of stablecoins is: the instrument may be novel, but the FEMA exposure is old and familiar.

PMLA Now Explicitly Covers VDA Exchanges

A March 2023 notification under PMLA expanded the definition of "Reporting Entity" to explicitly include Virtual Asset Service Providers (VASPs) — which covers any entity dealing in VDAs. This means VDA exchanges, wallets, and fintech platforms facilitating VDA transactions must comply with the full suite of PMLA KYC, record-keeping, and FIU-IND reporting obligations described in Part 6 of this article.

ADVISORY: Four Laws, One VDA Transaction

A single VDA transaction on your platform may simultaneously trigger:

(1) Income Tax Act — Section 194S: Deduct 1% TDS before releasing payment.

(2) FEMA — Section 4: Verify user is not holding foreign-currency-equivalent assets in

violation of FEMA.

(3) PMLA — Section 12: Record and monitor the transaction; report if above threshold or suspicious.

(4) RBI Caution Advisory (June 2021): The RBI has continued to warn consumers and businesses about the risks of VDA, and has indicated it may issue further regulatory guidance. Operate as if enhanced scrutiny is imminent.

Operating a VDA platform under only one or two of these frameworks is not compliance. It is partial compliance — a different, and arguably more dangerous, kind of exposure.

Part 8: Importing Foreign Technology — You Are Also Importing Compliance Obligations

Most fintech founders do not think of themselves as importers. Yet every payment to a foreign SaaS vendor — AWS, Stripe, Twilio, Salesforce, GitHub, Google Workspace — is an outward remittance under FEMA, subject to withholding tax requirements under the Income Tax Act, and potentially subject to Equalisation Levy. These are not year-end provisions. They are transaction-level obligations.

Form 15CA and 15CB — The Mandatory Gateway

Before making any foreign remittance, the Indian entity must, in most cases:

22. **File Form 15CA online** on the Income Tax portal (incometax.gov.in), declaring the nature of payment, applicable treaty, and tax treatment.
23. **Obtain Form 15CB from a Chartered Accountant** confirming the withholding tax rate applicable, the treaty benefit claimed (if any), and whether the payment qualifies as royalty, FTS, or business income.

Note: Form 15CB is not required for all payments — the rules specify categories. Payments below INR 5 lakh per year per payee for personal remittances, and certain specified categories, are exempt. But for most business-to-business foreign payments above INR 5 lakh, both forms are required before the bank will process the remittance.

CAUTION: Your Bank Will Block the Payment

Under RBI's guidelines to Authorised Dealer banks, a bank is required to verify that the appropriate 15CA/15CB documentation exists before processing a foreign remittance for business payments above the threshold. If your forms are not filed, the bank will refuse the remittance. This means your cloud provider doesn't get paid, your services may be suspended, and you may face late payment penalties with the vendor — all because of a compliance form your accounts team thought could wait until the end of the year.

The Classification Problem: Royalty vs. FTS vs. Business Income

The tax treatment of your foreign vendor payment depends entirely on how that payment is classified:

- **Royalty (Section 9(1)(vi) of Income Tax Act):** Payment for the use of patents, copyrights, trademarks, models, commercial equipment, or secret formulas. Withholding tax at 10–15% under most DTAAs — or 20% under domestic law if no treaty applies.
- **Fees for Technical Services or FTS (Section 9(1)(vii)):** Payment for managerial, technical, or consultancy services. Withholding at 10–20% depending on applicable treaty.
- **Business Income (Article 7 of DTAAs):** If the foreign vendor has no PE in India, the payment is typically not taxable in India at all — no withholding tax required. This is the most favourable treatment.

The Engineering Analysis Ruling — What It Does and Does Not Mean

The Supreme Court of India in Engineering Analysis Centre of Excellence Pvt Ltd v. Commissioner of Income Tax (2021) ruled that payment for purchase of off-the-shelf shrink-wrapped software (sold under standard end-user licence agreements to all customers without customisation) is business income — NOT royalty. This means no withholding tax is applicable if the foreign vendor has no PE in India.

This is a significant ruling — but it is also frequently over-applied. Here is what it does NOT cover:

- Custom software developed specifically for your company (likely royalty or FTS)
- API access where you receive underlying code or modify the software (potentially royalty)
- White-labelled products with code access or IP licence components (potentially royalty)
- Consulting or implementation services bundled with the software (FTS)

ADVISORY

Classify Each Foreign Vendor Annually: Maintain a register of all foreign vendor payments. For each vendor, document: (a) nature of service — royalty, FTS, or business income; (b) applicable treaty rate or domestic withholding rate; (c) Form 15CA/15CB status; (d) TDS deducted and deposited via Form 27Q. Your CFO must review this quarterly, not annually. One missed payment can result in the vendor being treated as your assessee-in-default for non-deduction of TDS — with interest at 1.5% per month and a penalty equal to the TDS amount.

Equalisation Levy — The Digital Tax on Foreign Advertising

India introduced Equalisation Levy in 2016 on online advertising services provided by non-residents (6%), and expanded it in 2020 to non-resident e-commerce operators (2%). The 2% expanded levy on e-commerce supply was withdrawn effective 1 August 2024 (Finance Act 2024). However, the original 6% levy on online advertising services remains in full force.

Practical impact: If you pay Google Ads, Meta Ads, LinkedIn Campaigns, or any other foreign digital advertising platform, 6% Equalisation Levy applies on that payment. If you make these payments through an Indian registered entity (e.g., Google India Pvt Ltd), verify whether the levy has already been factored into the invoice. If you pay the foreign parent directly, you are responsible for the levy deposit.

Part 9: Ten Red Flags That Your Fintech May Already Be Non-Compliant

Even without intent to break the rules, gaps emerge in how platforms are built. Here are ten operational warning signs that your compliance architecture has vulnerabilities:

24. **Customer funds sit in your operating account** — even briefly — rather than in a dedicated nodal or escrow account with an RBI-authorised scheduled commercial bank.
25. **You process international payments through a bank API** but have no formal agreement that identifies your platform as a regulated technology service provider and allocates KYC/AML responsibility.
26. **Your platform allows international money transfers** without collecting purpose-of-remittance declarations (Form A2 equivalent) from users.
27. **You have a Singapore, UAE, or UK holding entity** but all decisions, staff, contracts, and operations are in India — without a POEM, PE, or GAAR analysis ever being conducted.
28. **Your platform allows stablecoin holdings or token transfers** by Indian users without verifying LRS compliance or FEMA applicability.
29. **You have no automated system for deducting and depositing 1% TDS** under Section 194S on every VDA transfer your platform facilitates.
30. **Your foreign SaaS vendor payments are compiled for Form 15CA/15CB** once a year at the CA's office — not filed before each individual qualifying remittance.
31. **You have not designated and registered a PMLA Principal Officer** with FIU-IND (goaml.fiu.gov.in), despite processing cross-border payments above threshold.
32. **Your KYC collects PAN and Aadhaar at onboarding** but has no ongoing transaction monitoring, PEP screening, or sanction list verification in your payment processing infrastructure.
33. **No one on your team can identify, with confidence, which specific flows in your product** involve foreign exchange under FEMA and which regulatory rule applies to each flow.

CAUTION

The presence of even one red flag does not mean regulatory enforcement is imminent. But it does mean you have a known, documentable vulnerability. Regulators often discover non-compliance not through random audits, but through Suspicious Transaction Reports filed by banks, whistleblower complaints, partner disputes, or tax audits that reveal cross-border structures. Regulatory risk is not a probability question — it is a severity question.

Part 10: The Compliance Map — A Practical Step-by-Step Framework

Compliance is not a document you file once. It is an operational system you build into your product, your banking structure, your contracts, and your team's responsibilities. Here is a practical five-step framework:

Step 1: Map Every Cross-Border Value Flow

Draw a flow diagram — on paper, on a whiteboard, anywhere — that shows every point where money or value crosses India's border in your product. Be comprehensive: include customer deposits, settlement outflows, intragroup transfers to overseas entities, foreign vendor payments, and VDA transactions.

Step 2: Assign a Regulatory Label to Each Flow

For each flow, identify the applicable rule. Use this quick reference:

- **Indian resident sends money abroad** → LRS (USD 250,000 cap, TCS obligation, Form A2)
- **Indian platform collects and settles cross-border payments** → PA licence / PSS Act / nodal account requirements
- **Inward personal remittance from abroad** → MTSS framework or AD Category I bank authorisation
- **VDA trade or transfer** → Section 194S TDS, Section 115BBH income tax, FEMA Section 4, PMLA reporting
- **Payment to foreign SaaS/technology vendor** → Section 195 TDS, Form 15CA/15CB, Equalisation Levy (if advertising)
- **Intragroup transfer to overseas holding company** → FEMA Section 6, ODI rules, Transfer Pricing documentation

Step 3: Identify the Authorised Entity for Each Flow

For each flow, confirm: which party holds the licence or authorisation? Is it your AD Category I bank? Your Payment Aggregator partner (if you partner rather than self-licence)? Your own licence? If there is no licensed entity in the chain, that flow is non-compliant.

Step 4: Verify the Documentation Trail

For each flow, verify that the required documentation exists BEFORE the transaction:

- Form 15CA/15CB filed before each qualifying foreign vendor remittance
- Form A2 declarations from users initiating LRS remittances
- Nodal account agreement in place before any customer funds are collected
- KYC complete and current for all merchants/users

- TDS calculated, deducted, and deposited on schedule

Step 5: Establish Ongoing Monitoring — Not Just One-Time Checks

- Monthly review: LRS utilisation per user segment, TDS deductions and deposits
- Quarterly review: All foreign vendor payments for 15CA/15CB compliance; Transfer pricing positions
- Annual audit: PMLA framework audit; FEMA compliance review; PA licence conditions review
- Event-triggered review: Every time a new cross-border product feature is launched, before launch

> **PRACTICAL TIP: Create a Cross-Border Compliance Register**
>
> Build and maintain a single document — a spreadsheet or Notion database — that maps: (a) every cross-border transaction type your platform handles, (b) the applicable regulation, (c) the responsible team member, (d) the required documentation, (e) current status, and (f) date of last review. This single document will serve you in regulatory audits, investor due diligence, and RBI inspections better than any other compliance artefact.

Part 11: If You Are Already in the Grey Zone — What To Do Now

If you have read through this article and recognised gaps in your platform's compliance structure, here is the recommended course of action — in order of priority:

34. **Stop and Assess Before Fixing Anything:** Do not make impulsive changes to your product or financial structure without qualified legal advice. Attempting to retroactively fix a FEMA violation without guidance can itself trigger reporting requirements or create fresh evidence of deliberate non-compliance. Engage a specialist first.
35. **Engage a Specialist — Not a Generalist:** FEMA, PSS Act, and PMLA compliance is highly specialised. Your company secretary, general tax CA, or startup lawyer may not have sufficient depth. You need someone who has handled RBI licensing queries, FEMA compounding applications, or Payment System Operator processes at the RBI's DPSS.
36. **Consider Voluntary Compounding:** Under Section 15 of FEMA, contraventions can be "compounded" by the RBI or the Enforcement Directorate — meaning a penalty is accepted voluntarily in lieu of prosecution. The RBI's Master Direction on Compounding of Contraventions Under FEMA provides a structured process for voluntary disclosure. Going to the regulator proactively almost always results in a substantially better outcome than being discovered during an investigation.
37. **Fix the Product, Not Just the Legal Entity:** If your cross-border payment flow has a structural problem — customer funds pooling in an unlicensed account — the fix is at the product architecture level, not just the entity or contract level. Be prepared to redesign the payment flow itself.
38. **File Pending Compliance Documents Immediately:** If you have unresolved Form 15CA/15CB filings, un-deposited TDS under Section 194S, or unreported transactions to

FIU-IND, file and deposit immediately. Voluntary correction before a notice consistently attracts lower penalties than correction after a regulatory inquiry begins.

> **ADVISORY: Regulators Can See Your Cross-Border Transactions**
>
> The RBI receives transaction-level data from all AD Category I banks as part of the mandatory reporting system. TDS data from Section 194S flows into the Income Tax Department's automated systems. PMLA reports filed by banks go to FIU-IND, which shares intelligence with the Enforcement Directorate. The assumption that non-filing or informal arrangements are invisible to regulators is a founding-era myth that does not survive contact with a fintech that has scaled beyond a few hundred transactions per month.
>
> **Practical consequence:** At your current transaction volume, your cross-border payment flows are likely already visible to at least one regulator. The question is not whether they can see them — it is whether what they see is in order.

Conclusion: Build Compliance Before the Regulator Builds Your Case

The most expensive sentence in Indian fintech is: "We'll sort out the compliance when we raise the next round."

By the time you raise the next round, your investors' lawyers will conduct a legal and regulatory due diligence, and every one of these vulnerabilities will surface. The Singapore structure without GAAR analysis will become a condition precedent in your term sheet. The missing nodal account agreement will become a data room red flag. The pending 15CA filings will surface as a material liability in your M&A conversation.

More fundamentally, FEMA and PSS Act violations do not have a statute of limitations that works in your favour. They survive fundraising rounds, management changes, and ownership transfers.

Before you build the next cross-border feature, answer these five questions:

39. Does this feature involve cross-border movement of money or value?
40. What specific rule under FEMA / PSS Act / PMLA / Income Tax Act applies to this flow?
41. Which entity in my payment chain holds the licence or authorisation to enable this flow?
42. What documentation must be collected and filed — and when?
43. Who on my team owns this compliance item, and when was it last reviewed?

If you can answer all five with confidence and supporting documentation, build the feature. If you cannot, answer them first.

India is actively expanding its cross-border payment infrastructure — UPI-PayNow (India-Singapore), RBI's Project Nexus participation, CBDC pilots, and the international expansion of UPI to 10+ countries. This is a genuinely significant commercial opportunity for Indian fintechs. Those who capture it will be the ones who understood that international payments are not

merely a technology problem. They are a regulatory engineering problem — and the engineers who solve it correctly build durable, scalable, and globally respected businesses.

ADVISORY: About the Author

Dr. Anil Gupta is the Chairman of Connect Ventures Group of Companies, a TEDx Speaker, and a designated Mentor of Change by NITI Aayog, Government of India. Through his advisory practice, he has guided businesses across India, Singapore, UAE, and the United States on regulatory compliance, cross-border expansion strategy, and international business structuring.

He is the Founder of **Comply Globally** (complyglobally.com), which provides structured compliance and regulatory advisory services to businesses navigating cross-border growth — particularly Indian businesses expanding globally and international businesses entering the Indian market.